(Abstract:encryption and Abstract:strong) and (Abstract:cipher or Abstract:formula or Abstract:function or Abstract:algorithm)
Terms used: **encryption strong cipher formula function algorithm**

Found **23** of **248,815**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Open results in a new window

Refine these results with Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 23 Result page: 1 2 next >>

1 A methodology to implement block ciphers in reconfigurable hardware and its application to fast and compact AES RIJNDAEL

François-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater, Jean-Didier Legat

February 2003 FPGA '03: Proceedings of the 2003 ACM/SIGDA eleventh international symposium on Field programmable gate arrays

Publisher: ACM

Full text available: pdf(236.87 KB)

Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 14, Downloads (12 Months): 112, Citation Count: 3

Reprogrammable devices such as Field Programmable Gate Arrays (FPGA's) are highly attractive options for hardware implementations of encryption algorithms and this report investigates a methodology to efficiently implement block ciphers in CLB-based ...

Keywords: AES RIJNDAEL, FPGA, cryptography, high encryption rates, reconfigurable hardware

2 Authenticated encryption in SSH: provably fixing the SSH binary packet protocol

Mihir Bellare, Tadayoshi Kohno, Chanathip Namprempre
November 2002 CCS '02: Proceedings of the 9th ACM conference on Computer and communications security
Publisher: ACM
Full text available: pdf(287.08 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 99, Citation Count: 3

The Secure Shell (SSH) protocol is one of the most popular cryptographic protocols on the Internet. Unfortunately, the current SSH authenticated encryption mechanism is insecure. In this paper we propose several fixes to the SSH protocol and, using techniques ...

Keywords: SSH, authenticated encryption, secure shell, security proofs, stateful decryption

3 Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm

Mihir Bellare, Tadayoshi Kohno, Chanathip Namprempre
May 2004 ACM Transactions on Information and System Security (TISSEC), Volume 7 Issue 2
Publisher: ACM
Full text available: pdf(404.99 KB) Additional Information: full citation, abstract, references, index terms, review

Bibliometrics: Downloads (6 Weeks): 29, Downloads (12 Months): 157, Citation Count: 0

The *secure shell* (SSH) protocol is one of the most popular cryptographic protocols on the Internet. Unfortunately, the current SSH authenticated encryption mechanism is insecure. In this paper, we propose several fixes to the SSH protocol and, ...

Keywords: Authenticated encryption, secure shell, security proofs, stateful decryption

4 Universal strong encryption FPGA core implementation

D. Runje, M. Kovac
February 1998 DATE '98: Proceedings of the conference on Design, automation and test in Europe
Publisher: IEEE Computer Society
Full text available: pdf(157.43 KB) Publisher Site Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 16, Citation Count: 1

IDEA is a symmetric block cipher with a 128-bit key proposed to replace DES where a strong encryption is required. Many applications need speed of a hardware encryption implementation while trying to preserve flexibility and low cost of a software implementation. ...

Keywords: Encryption, Chip Architecture, IDEA, FPGA

5 A free, readily upgradeable, interactive tool for teaching encryption algorithms

Chris McNear, Chrisila C. Pettey
March 2005 ACM-SE 43: Proceedings of the 43rd annual Southeast regional conference - Volume 1, Volume 1
Publisher: ACM
Full text available: pdf(741.01 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 71, Citation Count: 0

There are rising concerns about data security in our society. Strong cryptographic systems provide a primary means of dealing with these concerns. Since encryption algorithms are an integral component of any cryptographic system, computer science students ...

Keywords: cryptography, decryption, encryption, simulator, teaching aid

6 Lower bounds on the efficiency of encryption and digital signature schemes

Rosario Gennaro, Yael Gertner, Jonathan Katz
June 2003 STOC '03: Proceedings of the thirty-fifth annual ACM symposium on Theory of computing
Publisher: ACM
Full text available: pdf(236.93 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 62, Citation Count: 0

A central focus of modern cryptography is to investigate the weakest possible assumptions under which various cryptographic algorithms exist. Typically, a proof that a "weak" primitive (e.g., a one-way function) implies the existence of a "strong" algorithm ...

Keywords: black-box, digital signatures, encryption, lower bounds

7 An FPGA implementation and performance evaluation of the Serpent block cipher

A. J. Elbirt, C. Paar
February 2000 FPGA '00: Proceedings of the 2000 ACM/SIGDA eighth international symposium on Field programmable gate arrays
Publisher: ACM
Full text available: pdf(674.09 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 103, Citation Count: 10

With the expiration of the Data Encryption Standard (DES) in 1998, the Advanced Eneryption Standard (AES) development process is well underway. It is hoped that the result of the AES process will be the specification of a new non-classified encryption ...

Keywords: FPGA, VHDL, algorithm-agility, block cipher, cryptography

8 Designing encryption algorithms for real people

Bruce Schneier
August NSPW '94: Proceedings of the 1994 workshop on New security paradigms 1994
Publisher: IEEE Computer Society Press
Full text available: pdf(332.46 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 65, Citation Count: 0

There is a wide disparity between cryptographic algorithms as specified by researchers and cryptographic algorithms as implemented in software applications. Programmers are prone to implement poor key management, make mistakes coding the algorithm, and ...

9 Side-channel attack pitfalls

Kris Tiri
June DAC '07: Proceedings of the 44th annual conference on Design automation 2007
Publisher: ACM
Full text available: pdf(331.31 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 18, Downloads (12 Months): 167, Citation Count: 0

While cryptographic algorithms are usually strong against mathematical attacks, their practical implementation, both in software and in hardware, opens the door to side-channel attacks. Without expensive equipment or intrusive monitoring, these attacks ...

Keywords: differential power analysis, encryption, security IC, side-channel attack

10 Architectural support for fast symmetric-key cryptography

Jerome Burke, John McDonald, Todd Austin
December 2000 ACM SIGOPS Operating Systems Review, Volume 34 Issue 5
Publisher: ACM
Full text available: pdf(160.25 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 32, Downloads (12 Months): 171, Citation Count: 21

The emergence of the Internet as a trusted medium for commerce and communication has made cryptography an essential component of modern information systems. Cryptography provides the mechanisms necessary to implement accountability, accuracy, and confidentiality ...

11 Cryptographic strength of ssl/tls servers: current and recent practices

Homin K. Lee, Tal Malkin, Erich Nahum
October 2007 IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement
Publisher: ACM
Full text available: pdf(188.49 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 45, Downloads (12 Months): 304, Citation Count: 0

The Secure Socket Layer (SSL) and its variant, Transport Layer Security (TLS), are used toward ensuring server security. In this paper, we characterize the cryptographic strength of public servers running SSL/TLS. We present a tool developed for this ...

Keywords: network security, servers, ssl

12 Trusted declassification:: high-level policy for a security-typed language

Boniface Hicks, Dave King, Patrick McDaniel, Michael Hicks
June 2006 PLAS '06: Proceedings of the 2006 workshop on Programming languages and analysis for security
Publisher: ACM
Full text available: pdf(301.18 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 105, Citation Count: 4

Security-typed languages promise to be a powerful tool with which provably secure software applications may be developed. Programs written in these languages enforce a strong, global policy of *noninterference*which ensures that high-security data ...

Keywords: *noninterference modolo trusted methods*, FJifP, Jif, declassification, information-flow control, security policy, security-typed languages, trusted declassification

13 Architectural support for fast symmetric-key cryptography

Jerome Burke, John McDonald, Todd Austin
November 2000 ACM SIGPLAN Notices, Volume 35 Issue 11
Publisher: ACM
Additional Information: full citation, abstract, cited by, index terms

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 1

The emergence of the Internet as a trusted medium for commerce and communication has made cryptography an essential component of modern information systems. Cryptography provides the mechanisms necessary to implement accountability, accuracy, and confidentiality ...

14 Cryptography with constant computational overhead

Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Amit Sahai

May 2008 STOC '08: Proceedings of the 40th annual ACM symposium on Theory of computing

Publisher: ACM

Full text available: pdf(286.14 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 46, Downloads (12 Months): 46, Citation Count: 0

Current constructions of cryptographic primitives typically involve a large multiplicative computational overhead that grows with the desired level of security. We explore the possibility of implementing basic cryptographic primitives, such as encryption, ...

Keywords: constant computational overhead, cryptography, universal hashing

15 Revealing skype traffic: when randomness plays with you

Dario Bonfiglio, Marco Mellia, Michela Meo, Dario Rossi, Paolo Tofanelli

August 2007 SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications

Publisher: ACM

Full text available: pdf(911.54 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 116, Downloads (12 Months): 667, Citation Count: 0

Skype is a very popular VoIP software which has recently attracted the attention of the research community and network operators. Following a closed source and proprietary design, Skype protocols and algorithms are unknown. Moreover, strong encryption ...

Keywords: deep packet inspection, internet traffic identification, naive bayesian classification, passive measurement, pearson chi-square test

16 Secure and practical defense against code-injection attacks using software dynamic translation

Wei Hu, Jason Hiser, Dan Williams, Adrian Filipi, Jack W. Davidson, David Evans, John C. Knight, Anh Nguyen-Tuong, Jonathan Rowanhill

June 2006 VEE '06: Proceedings of the 2nd international conference on Virtual execution environments

Publisher: ACM

Full text available: pdf(270.13 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 19, Downloads (12 Months): 160, Citation Count: 2

One of the most common forms of security attacks involves exploiting a vulnerability to inject malicious code into an executing application and then cause the injected code to be executed. A theoretically strong approach to defending against any type ...

Keywords: software dynamic translation, virtual execution

17 Architectural support for fast symmetric-key cryptography

Jerome Burke, John McDonald, Todd Austin
November 2000 ASPLOS-IX: Proceedings of the ninth international conference on Architectural support for programming languages and operating systems
Publisher: ACM
Full text available: pdf(160.25 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 32, Downloads (12 Months): 171, Citation Count: 21

The emergence of the Internet as a trusted medium for commerce and communication has made cryptography an essential component of modern information systems. Cryptography provides the mechanisms necessary to implement accountability, accuracy, and confidentiality ...

18 Architectural support for fast symmetric-key cryptography

Jerome Burke, John McDonald, Todd Austin
December 2000 ACM SIGARCH Computer Architecture News, Volume 28 Issue 5
Publisher: ACM
Full text available: pdf(160.25 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 32, Downloads (12 Months): 171, Citation Count: 21

The emergence of the Internet as a trusted medium for commerce and communication has made cryptography an essential component of modern information systems. Cryptography provides the mechanisms necessary to implement accountability, accuracy, and confidentiality ...

19 Public-key cryptography and password protocols

Shai Halevi, Hugo Krawczyk
August 1999 ACM Transactions on Information and System Security (TISSEC), Volume 2 Issue 3
Publisher: ACM
Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, cited by, index terms, review

Bibliometrics: Downloads (6 Weeks): 38, Downloads (12 Months): 355, Citation Count: 11

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

20 Enhanced Skype traffic identification

Marcell Perényi, Sándor Molnár
October 2007 ValueTools '07: Proceedings of the 2nd international conference on Performance evaluation methodologies and tools
Publisher: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)
Full text available: pdf(361.65 KB) Additional Information: full citation, abstract, references

Bibliometrics: Downloads (6 Weeks): 26, Downloads (12 Months): 116, Citation Count: 0

Skype applies strong encryption to provide secure communication inside the whole Skype network. The communication ports of clients are chosen randomly. As a consequence, traditional port based or payload based identification of Skype traffic cannot be ...

Keywords: Skype, analysis, traffic identification

Results 1 - 20 of 23 Result page: 1 2 next >>